PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-111745

(43)Date of publication of application : 12.04.2002

(51)Int.Cl. H04L 12/66
H04L 12/46
H04L 12/28
H04L 12/56

(21)Application number : 2000-302819

(22)Date of filing : 29.09.2000

(71)Applicant : HITACHI LTD

(72)Inventor : NAMIOKA YOSHIMITSU
MIYAO TAKESHI
NAKANO TOSHIHIKO

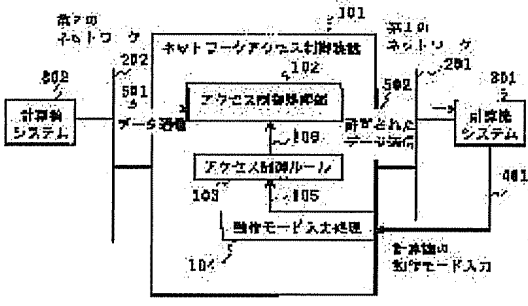
(54) NETWORK ACCESS CONTROL DEVICE, ITS CONTROL METHOD, ITS CONTROL SYSTEM AND COMMUNICATION SERVICE METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a means for confirming services available at the time of maintenance for each calculator by a maintenance crew himself when he maintains the calculators from a remote place and to enable a network access control device to control the passage or the non permission of communication data according to the operation mode of a plurality of calculators.

SOLUTION: The network access control device is set up at an access point between a calculator which can be maintained from a remote place and an external network. The network access control device is provided with operation modes corresponding to access control rules of the calculator. When there are a plurality of

図 1



calculators, each of them is provided with an operation mode.

CLAIMS

[Claim(s)]

[Claim 1]A network access control apparatus which performs communications control between computers connected to a network, comprising:

The access control rule Management Department which makes the mode in which an operation plan applied to an access control rule which controls data which communicates between connected networks, and a computer to manage is expressed correspond, and manages.

A connection management department which manages a connection according to it with the application of an access control rule corresponding to the mode applied to this computer.

A data communication part which transmits commo data among two or more networks only when a connection is permitted.

[Claim 2]After cancelling an access control rule applied collectively in claim 1, A network access control apparatus having a connection management department which bundles up an access control rule corresponding to the specific mode, and is validated out of two or more access control rules prepared beforehand.

[Claim 3]A network access control apparatus having a connection management department which continues a connection about an already established connection even if it is a candidate for cancellation when changing an access control rule applied collectively in claim 2.

[Claim 4]In a network access control method which controls data communications between computers connected to a network, A network access control method which applies to a computer which manages the mode in which correspond to an access control rule which specifies data-communications conditions, and an operation plan is expressed, tests an access control rule corresponding to this mode, and received data by comparison, judges a passing permission, and sends out data.

[Claim 5]In a network access control method which controls data communications between computers connected to a network, A mode conversion table to which the mode in which an operation plan applied to an access control rule which controls data transmitted between connected networks, and a computer to manage is expressed is made to correspond, A network access control method which is based without a

computer conversion table to which a computer to manage and this mode are made to correspond, judges a passing permission of received data, and sends out or cancels this data.

[Claim 6]In a network access control system which controls data communications between computers connected to a network, It applies to a computer which manages the mode in which correspond to an access control rule used as a standard of data-communications judgment, and an operation plan is expressed, A network access control system which controls communication by testing by comparison data received from an access control rule and an external computer corresponding to this mode, judging a passing permission, and sending out data to a computer to manage.

[Claim 7]A network access control system which makes two or more computers and these modes to manage correspond in claim 6, and controls data communications based on it.

[Claim 8]It is the remote maintenance service provision method performed by remote control via a network access control apparatus which controls data communications between computers connected to a network, A remote maintenance service provision method that a service beneficiary responds to the mode in which an operation plan set as a network access control apparatus is expressed, and maintains or manages a computer with service which can communicate in this mode.

[Claim 9]It is the remote maintenance service provision method performed by remote control via a network access control apparatus which controls data communications between computers connected to a network, A remote maintenance service provision method that a service beneficiary responds to the mode in which an operation plan to a computer set as a network access control apparatus is expressed, and maintains or manages two or more computers with service which can communicate in this mode.

[Claim 10]It is the remote maintenance service provision method performed by remote control via a network access control apparatus which controls data communications between computers connected to a network, A remote maintenance service provision method that a service beneficiary displays this mode or an operation plan on a screen of a purveyor's of service computer, and maintains or manages a computer according to the mode in which an operation plan to a computer set as a network access control apparatus is expressed.

[Claim 11]A remote maintenance service provision method displaying a service content on a maintenance service screen in claim 10.

[Claim 12]A remote maintenance service provision method displaying a computer maintained or managed on a maintenance service screen in claim 10.

[Claim 13]A remote maintenance service provision method that the mode includes the above in claims 8 thru/or 12 even in one inside of an initial mode, online mode, maintenance mode, a test mode, and monitor run mode.

[Claim 14]A remote maintenance service provision method of charging a maintenance service fee in claims 8 thru/or 13 according to the mode applied to a computer.

[Claim 15]A remote maintenance service provision method characterized by charging for every computer when charging a maintenance service fee in claims 8 thru/or 13 according to the mode applied to a computer.

[Claim 16]A remote maintenance service method which is a remote maintenance service method between computers which communicate via a network access control apparatus, continues communication and provides service until it establishes a connection between computers and communication is completed, even if a service beneficiary changes an access control rule during communication.

[Claim 17]A contents distribution service method of continuing communication established during this period even if it passed over a shelf-life when setting up and carrying out service provision of the shelf-life to distribution service in a contents distribution service between computers which communicate via a network access control apparatus, and providing service.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to a network access control apparatus and a method, a system, and a remote maintenance service method.

[0002]

[Description of the Prior Art]This kind of access control art is conventionally realized as a product called a router and a firewall. The rule for carrying out access control beforehand is set up, and the passing permission or disapproval of commo data is controlled by conventional technology according to the rule. The method with which the rule specifies the passing permission or disapproval of commo data based on the network address of the computer of a transmission destination is known widely.

[0003]About the art which maintains a computer from remoteness, maintenance mode is provided in a computer as operational mode, Maintenance mode is judged for this computer itself, the commo data permitted by maintenance mode is received, and the access control art of keeping a computer from receiving mistaken data by not receiving

the commo data which is not permitted is widely known for maintenance mode.

[0004]The packet-filtering device which transmits to the conventional network access control apparatus based on the regulation which is a unit of the data which communicates between computers, and which investigated the destination or the source for every packet, and was given beforehand is known widely. It specializes in the operating application program which communicates, regulation of a communication condition is established to the communication procedure of data, or the kind of data which communicates, and the communication vicarious execution device which transmits based on it is known widely.

[0005]As a device which changes dynamically the rule which specifies transmission propriety, each rule was applied to JP,11-167538,A one by one like a statement.

[0006]

[Problem(s) to be Solved by the Invention]However, if the maintenance mode for applying a rule is set up by each computer, setting out is complicated, and about the computer which cannot set up maintenance mode, a rule must be set up by a firewall. In access control rule management, it is a technical problem to enable it to identify the purpose of the access control rule which carries out grouping of two or more rules as one access control rule, and is applied to the present network access control apparatus.

[0007]And when setting up a rule in the access control to two or more computers, it is hard to hold which computers are what kind of operation plan and a security policy. Therefore, in a network access control apparatus, it is a technical problem to control passage of commo data or disapproval to two or more computers according to the operational mode of this computer.

[0008]When maintaining a computer from a remote place, it is a technical problem to provide a means by which the service which a customer engineer can use at the time of a maintenance service can be checked for every computer for customer engineer itself.

[0009]

[Means for Solving the Problem]In order to solve an aforementioned problem, a network access control apparatus is formed in a connection point of a computer and an external network which make it possible to perform maintenance from remoteness, and operational mode corresponding to an access control rule of this computer is provided in this network access control apparatus. In the case of a computer which consists of two or more computers, operational mode is provided to each computer.

[0010]Service which can be used via a network access control apparatus at the time of a maintenance service is displayed for each computer of every from operational mode which a network access control apparatus holds, and an access control rule.

[0011]

[Embodiment of the Invention]As Example 1 of this invention, the operational mode of a computer is inputted and the example which carries out access control according to this mode is shown in drawing 1. The computer (301) connected to the 1st network (201) and the 1st network, The computer (302) connected to the 2nd network (202) and the 2nd network exists, and a network access control apparatus (101) is the composition of having connected the 1st network (201) and 2nd network (202). A network access control apparatus (101) consists of an access control treating part (102), an access control rule (103), and an operational mode input processing part (104). An access control treating part (102) receives data from the computer connected to the 2nd network (501), It checks by an access control rule (105) (106), it judges [of this data] whether a passing permission should be carried out, and when carrying out a passing permission, data is transmitted to the computer (301) connected to the 1st network (502). A network access control apparatus (101) has an operational mode input processing part (104) for inputting the operational mode of a computer, and inputs the operational mode of a computer (301) to this computer connected to the 1st network (401). An access control rule is changed into these operational modes according to the inputted operational mode (105). By this method, control of the passing permission of commo data or disapproval can be carried out in a network access control apparatus according to the operational mode of the computer (301) connected to the 1st network. For example, by online mode, it becomes possible to the computer (301) of online mode to make the commo data for an examination which is not processed discard with a network access control apparatus.

[0012]The access control rule (103) before and behind an access control treating part [in / here / drawing 1] (102) and change is realized with the composition shown in drawing 2. In a network access control apparatus (101), an access control treating part (102-1) comprises a data communication part (102-2) and a connection management department (102-3). A data communication part (102-2) from the computer (302) connected to the 2nd network (202). The connection (404) established with the network access control apparatus (101) in order to transmit the data which should be transmitted to the computer (301) connected to the 1st network (201), And in order to transmit the data which the network access control apparatus (101) received to a computer (302), bidirectional communication is relayed to a computer (302) through the established connection (403). A connection management department (102-3) controls connection of a connection based on the access control rule (103-4) as which the establishment propriety conditions of the connection were specified.

[0013]The access control rule (103) shown by drawing 1 is realized at the access control

rule Management Department (103-1) of drawing 2. The access control rule Management Department (103-1) holds two or more access control rules (103-3) with an identifier (103-2).

[0014]Operation of the real original form voice shown in drawing 2 is explained. An access control rule (103-3) is prepared beforehand first. An access control rule The IP address and port number of a data transmission former computer, And the IP address and port number of a transmission destination computer which transmit the IP address which receives a connection with the network access control apparatus (101) by which this invention is carried, a port number, and the received data are described. These description permits establishment of a connection clearly and the connection to which an IP address or a port number does not correspond to a descriptive content refuses the establishment request of a connection tacitly. An identifier (103-2) is given to an access control rule.

[0015]The description format of the access control rule (103) in drawing 1 is shown in drawing 3. The identifier (111) an access control rule indicates the classification of a protocol to be, The IP address (112) and port number (113) of a computer which permit establishment of a connection, The IP address (116) and port number (117) of a computer which serve as a transmission destination of data which received with the IP address (114) and the port number (115), IP address (114), and port number (115) which a network access control apparatus receives are comprised.

[0016]In drawing 2, one or more access control rules (103-3) are created in accordance with the state of a computer (301) or a computer (302), and give an identifier (103-2). For example, if the operational mode of a computer (301) is on-line, it will be considered as the access control rule to which a connection is permitted only from a computer (302) to be communicated, and the identifier which shows "online mode" will be given. For example, if the operational mode of a computer (301) is a maintenance state, it will be considered as the access control rule to which a connection is permitted only to the specific port of a computer (301) from a computer (302), and the identifier which shows "maintenance mode" will be given. For example, if the operational mode of a computer (301) is test mode, it will be considered as the access control rule to which communication required for an examination is permitted, and the identifier which shows "test mode" will be given.

[0017]The access control rule Management Department (103-1), With a system administrator or the directions from other programs, for example, the access control rule changing instruction in drawing 1, (105). The specific access control rule (103-4) which has the specified identifier out of the access control rule currently held is shown

to a connection management department (102-3).

[0018]A connection management unit (102-3) validates the access control rule (103-4) which should apply the contents of the access control rule applied till then to the next after repealing all. Here, the connection shall be continued unless either a computer (301) or a computer (302) cuts a connection clearly, in becoming invalid [the connection already established when the last access control rule became invalid].

[0019]When there is a demand of a connection from a computer (302) to a network access control apparatus (101), a connection management department (102-3), The IP address of a computer (302) and the information on a port number which are included in the demand are acquired, and description with which the IP address (112) shown in drawing 3 and a port number (113) agree out of the access control rule (103-4) which is effective now is searched. A connection demand is refused when there is no agreeing description. When agreeing description exists, a connection management department (102-3) establishes a connection to the IP address (116) and port number (117) of a destination computer which are shown in drawing 3 in searched description. Henceforth, a data communication part (102-2) relays the data received through the connection which continued the connection (403) and the connection (404) and was established until either the computer (301) of drawing 2 or a computer (302) cuts a connection clearly.

[0020]The access control rule Management Department (103-1) presents the identifier of the access control rule (103-4) which the connection management unit has applied with a system administrator or the directions from other programs.

[0021]Not only a single port number but the method which realizes data communications from the communication middle like FTP using arbitrary port numbers exists in a data communication system. The operation in that case is shown in drawing 4. When a computer (301) and a computer (302) communicate, a computer (302) establishes a connection to the specific port number of a network access control apparatus (100) (210-2). A network access control apparatus (100) establishes a connection with a computer (301) according to an access control rule (210-1). A computer (301) transmits usable arbitrary port numbers to a network access control apparatus (100) now (211-1). As for a network access control apparatus (100), self transmits usable arbitrary port numbers to a computer (302) like a computer (301) now (211-2). Here a network access control apparatus (100), By permitting a connection demand in the arbitrary ports usable now which self chose, even when the computer (302) has required the connection from a previous port number, a connection can be established continuously.

[0022]As Example 2 of this invention, the example which applied maintenance mode as operational mode of a computer is shown in drawing 5. The computer 1 (301-1), the computer 2 (301-2), and the computer 3 (301-3) are connected to the 1st network (201), and a computer has operational mode, respectively. The operational mode of the computer 1 (301-1) is maintenance mode, and inputs the information on this operational mode into the operational mode input processing part (104) of a network access control apparatus (101) (401-1). The operational mode of the computer 3 (301-3) is online mode, and inputs the information on this operational mode into the operational mode input processing part (104) of a network access control apparatus (101) (401-2). When the computer (302) connected to the 2nd network carries out data communications to the computer 1 connected to the 1st network, in a network access control apparatus (101). the case where it is the data which judged whether it was the data permitted to the computer of maintenance mode according to the access control rule (103), and was permitted -- as long as -- data communications are carried out to the computer 1 (502). Similarly it judges whether when carrying out data communications to the computer 3, it is the data permitted to the computer of online mode, and when it is the permitted data, it restricts and data communications are carried out to the computer 3.

[0023]As Example 3 of this invention, the example of mounting of a network access control apparatus is shown in drawing 6 - drawing 7. A network access control apparatus (101) consists of an access control treating part (102), an access control rule (103), and an operational mode input processing part (104). An access control treating part consists of a program (102-4) which performs access control. An access control program (102-4) receives the data from the outside (501), The data which described the access control rule is read (106), this rule and commo data are tested by comparison, in the case of the permitted data, data is relayed (502), and, in the case of the data which is not permitted, data is discarded. An operational mode input processing part (104) consists of an operational mode input program (104-1), is the operational mode input (401) waiting from a computer, and can input operational mode at any time. If operational mode is inputted from a certain computer, an access control rule will be changed into an access control rule reflecting the information on this operational mode (105). Drawing 7 is an example of the data format (401-3) from a computer to the operational mode input processing part for inputting operational mode. It consists of the network address (401-4) of a transmitting agency computer, a network address (401-5) of a network access control apparatus, and operation mode information of a transmitting agency computer. A computer can be specified by the network address (401-4) of a transmitting agency computer. Operational mode is specified by the

operation mode information (401-6) of a transmitting agency computer. As an example of operational mode, online mode, maintenance mode, a test mode, etc. are mentioned.

[0024]As Example 4 of this invention, a computer is shown in drawing 8 about the access control system in the case of carrying out remote maintenance. A network access control apparatus (101) inputs operational mode (401) from the computer (301) connected to the 1st network (201), and changes an access control rule (103) by this operational mode. The computer (302) connected to the 2nd network (202) inputs operational mode (401) and an access control rule (103) from a network access control apparatus (101) (402). A computer (302) searches the rule which agrees out of an access control rule (103) in the IP address (112) of the transmitting agency computer which the IP address of the computer (302) showed by drawing 3, The IP address (116) and port number (117) of a transmission destination computer which were further shown by drawing 3 are extracted from these search results, and a service list (511) is created. In other words, the extracted information shows the service which a customer engineer can use by maintenance respectively via a network access control apparatus (101) about the computer (301) which can communicate, and a different computer (303). A customer engineer peruses the use propriety of service on the maintenance screen (512) displayed based on the service list. The composition and operation of a maintenance screen (512) are explained in drawing 9. A maintenance screen (512) consists of an operational mode indicator (521), a computer indicator (522), and a service indicator (523). The operational mode inputted from the network access control apparatus (101) shown by drawing 8 is displayed on an operational mode indicator (521). The IP address obtained by the service list shown by drawing 8 is displayed on a computer indicator (522). When a service list (522) has two or more computers, two or more IP addresses are displayed. A customer engineer carries out selection operation of the single IP address from a computer indicator (511). The port number obtained from the service list (511) shown by drawing 8 about the selected IP address is displayed on a service indicator (523). When there are two or more port numbers about the IP address which the customer engineer chose into the service list (511), two or more port numbers are displayed.

[0025]About Example 4 of this invention, the computer name which was beforehand defined as the IP address by relating in addition to the IP address may be displayed about a computer list display part (522). The service name which was beforehand related with the port number in addition to the port number may be displayed about a service indicator (523). An access control rule (103) is holding by a computer (302) beforehand, may input only operational mode from a network access control apparatus (101) (402), and may create a service list (511). After inputting the IP address of a

computer (302) to a computer (302), a service list (511) can be created with a network access control apparatus, and the computer (302) can also display a maintenance screen (512) by transmitting to a computer (302).

[0026]Drawing 10 is an example of the whole system by the side of service provision and service enjoyment about remote maintenance service. There are a certain equipment and a computer which controls it, and it is connected through the communication line via the network access control apparatus to the exterior. And the computer by the side of maintenance service can communicate now to a computer or equipment via a maintenance service server or a network access control apparatus. Remote maintenance services are the maintenance control work of equipment, repair, an offer of information which are provided with the protocol corresponding to a port, and the application of the protocol. When equipment of A company and B company is used on the occasion of management by outsourcing, setting out and employment can be simply performed by setting up the mode corresponding to each company to manage in each company. As equipment, industrial plants, such as power generation equipment and a factory production line, etc. are mentioned.

[0027]Drawing 11 is an example of a flow when giving its service. Online mode is set as the computer by the side of service enjoyment, a process control is performed by this, and equipment starts operation. The mode set as the computer is registered into a network access control apparatus. This registering operation transmits to a network access control apparatus from a computer, when the mode is set as a computer (601). And it tells that the contents of registration to the network access control apparatus changed to a maintenance service server, and registers (602). Since plant control is performed by the usual operational status in online mode, the communications control rule is set up change the state of the computer currently controlled and not risk a fatal mistake. A customer engineer performs the maintenance which is possible in the registered online mode. Here, it is supervisory service and it is being supervised whether it is normal (604). When equipment breaks down, a computer detects that equipment broke down and it is changed from online mode to maintenance mode. The control rule is set up be in the state where work for maintenance mode to make operation of computers, such as exchange of a program and change of data, changing can be performed. A computer registers a mode change into a network access control apparatus (605), and a network access control apparatus registers the mode change of a computer to a maintenance service server (606). It gets to know that the customer engineer which this was supervising by online mode until now checked that registration had been changed to maintenance mode (607), and was abnormal, maintenance

inspection which is possible in maintenance mode is conducted, and the result is reported (608).

[0028]Although registered with the degree of a mode change to the maintenance service server here, when communicating without registering, the information on the mode may be communicated.

[0029]When keeping maintenance mode data from going to computers other than maintenance mode, it can protect from remoteness that those who were permitted operation transmit commo data to computers other than maintenance mode accidentally.

[0030]Although what a computer detects that equipment broke down as was mentioned, in the surveillance of maintenance service, abnormalities other than the input by authorized personnel are checked, and it may enable it to change the mode of a computer to the maintenance computer by the side of maintenance service. At this time, since the mode in the network access control apparatus which is a firewall will be treated, also when other encoding technology needs to be used together from a viewpoint of security, it thinks. Thereby in a network access control apparatus, an access control rule can be changed without operation of the administrator of this device.

[0031]Drawing 12 shows an example of the charging method of the fee of maintenance service. If the mode is set up and maintenance service is requested, the maintenance service offer side will perform maintenance control in the service which is possible in the mode. The fee per time to be for every service is decided, and from the time spent with the service, a fee is determined and is charged. Since a service content changes by changing the mode, the fee corresponding to the service can receive to receive service to receive. A fee may be changed for every computer by forming the mode for every computer. As other charging methods, fixed time, such as a monthly contract, has the method of using as a fixed fee.

[0032]It is made to correspond like drawing 13 as an example to which a rule and the mode are made to correspond, and is managed with a network access control apparatus. It can be necessary to stop setting up the mode by each computer, and only information required for each computer can be passed by applying a rule with a network access control apparatus by making a rule and the mode correspond and managing with a network access control apparatus. Therefore, since it becomes unnecessary to judge whether it is required information by each computer, the load of each computer decreases. By forming two or more modes in which an operation plan is expressed, a rule to apply by changing an operation plan can be replaced without time and effort at once.

[0033]It is made to correspond like drawing 14 as an example to which each computer

and its mode are made to correspond, and is managed with a network access control apparatus. By setting up the mode for every computer, a rule is [that it is easy to grasp the operation plan of each computer] easily applicable. It can also be checked whether the access control rule for every operational mode is appropriately defined from one computer to two or more computers. By making some computers into the same computer group on an operation plan, and making them correspond with the mode, it can also collect as an operation plan of the system of a computer group.

[0034]The following is mentioned as a typical example in the mode.

(1) Initial mode : the state where business oriented applications (plant control program etc.) are not performed when a computer is started. From this state, it changes to other modes.

(2) Online mode : business oriented application is started and perform plant control. The usual operational status.

(3) Maintenance mode : the state which can perform the work for making operation of computers, such as exchange of a program, and change of data, change.

(4) Test mode : the state where a computer does not issue final control instruction. Data receiving from control machinery and transmission of control instruction are performed in false. It is used at the time of an operation test.

(5) Monitor run mode : the state which is received from the plant where the data receiving from control machinery is actual unlike a test mode. It is used at the time of an operation test.

[0035]Since the access control rule over the computer managed by changing two or more modes or the computer to maintain can be changed, a rule is easily applicable, grasping a management operation plan.

[0036]Maintenance service needs to create the required mode suitably and to carry out various services regardless of the mode and the service content which were mentioned as the example.

[0037]Drawing 15 is an example showing the flow of rule package application. When changing a network access control apparatus from a certain mode to another mode, three new rules are applied. When the connection demand from the outside is coming, three rules are applied one by one, but the upper row is a case where package application of the rule is not carried out, and the lower berth is a case where package application of the rule is carried out. When the communication A and the communication C are needed in communication with the exterior, in the state of [B] the state A of the upper row, the communication A establishes a connection, and can communicate, and the communication C has not established the connection. On the

other hand, when carrying out package application of the rule of the lower berth, since communication is started after the rule set by the mode is applied, the compatibility of communication of the communication A and the communication C is good. By validating collectively the mode which is an identifier showing an operation plan to apply, and two or more corresponding access control rules, after cancelling the access control rule applied to the managed computer collectively, When an access control rule comprises two or more rules, an access control rule can be made to change dynamically, without generating the transient state by changing each access control rule one by one.

[0038]Drawing 16 is an example of rule application and connection continuation. If the connection demand from the outside comes, a parent process judges communication propriety with the rule set in the mode applied to the computer of the communication destination, and if communication is good, it will pass communicative work to a child process. A child process establishes a connection to a connection demand, it communicates, and after communication is completed, it closes it. If a child process may be generated when receiving the communication which is work from a parent process, there may be from the beginning.

[0039]As the parent process was applied [the rule set of the communication destination computer], when it has a connection demand, since a rule set finishes being applied, it can carry out package application of the rule by delivering work to a child process. Once a child process establishes a connection, if it continues and closes communication until it closes a connection, it will be in the state of the waiting for work to a parent process. As the communication which established the connection is communication, it becomes impossible to communicate by closing of the connection by a rule interchanging by not carrying out rule application in the middle of communication.

[0040]In the packet-filtering device using conventional technology. Since transmission of a packet is no longer performed when the access control rule which refuses communication is applied, an operating application program may have to detect that transmission was interrupted and a series of processings of all to data till then or it may have to be repealed. However, about the already established connection, when changing the access control rule applied, even if it is a candidate for cancellation, the continuity of processing can be secured by continuing a connection. Thereby, by changing an access control rule collectively, communication can be continued and service can be provided until it establishes the connection between computers and communication is completed, even if it changes an access control rule during communication.

[0041]In remote maintenance service, in the case of the method of charging courtesy rates as a service period in time after a communicative connection is established until it

closes, if a connection is cut in the middle of maintenance service work, the work to the middle must become useless and must redo again. At this time, as a maintenance service offer side, the number of time and effort of work will increase, and fees will increase in number according to increase of working hours as a service enjoyment side. When setting the period which provides contents in the service which distributes data from a content provider by a music distribution etc. and charging it, in the service provision side, it is possible to change a rule with the end of the service period of a client, but. When the client which is a service enjoyment side has established the connection from just before a distribution service term, the communication will become useless if a connection is cut in the middle of communication. Package application of the rule is carried out, by making a connection continue, more positive communication can be provided in maintenance service or distribution service, better service can be provided, and fee collection corresponding to service can also be carried out.

[0042]

[Effect of the Invention]According to this invention, when maintaining a computer from remoteness, there is an effect to prevent about judging that in other words a computer is [whose computer is maintenance mode] in the state which can be maintained, and transmitting the data for maintenance to computers other than maintenance mode accidentally with a network access control apparatus.

[0043]It is that the service which becomes easy [a system administrator] to check the access control rule under application since the access control rule under present application can be interpreted semantically, and can be used now is shown in a customer engineer, and is effective in not doing trial work for investigating whether its service can be given.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]System configuration figure.

[Drawing 2]Composition of an access control treating part and the access control rule Management Department.

[Drawing 3]The data format of an access control rule.

[Drawing 4]The communication method which uses two or more ports.

[Drawing 5]The figure of the computer which consist of computers.

[Drawing 6]Composition of a network access control apparatus.

[Drawing 7]Communication data format.

[Drawing 8]The access control system in remote maintenance work.

[Drawing 9]Composition of a maintenance screen.

[Drawing 10]General drawing of remote maintenance service.

[Drawing 11]The flow by the side of maintenance service and service enjoyment.

[Drawing 12]The flow of the fee collection of maintenance control courtesy rates.

[Drawing 13]The conversion table of operational mode and an access control rule.

[Drawing 14]The conversion table of a computer and operational mode

[Drawing 15]The flow of rule package application.

[Drawing 16]The example of rule application and connection continuation.

[Description of Notations]

101 -- A network access control apparatus, 102 -- Access control treating part, 103 -- An access control rule, 104 -- An operational mode input processing part, 105 -- Rule change, 106 -- Data read, 201-202 -- A network, 210 -- Connection establishment, 211 -- Port number transmission, 212 -- Communication, 301-302 -- Computer, 401-402 -- The input of operational mode, 501-502 -- Data communications, 511 -- A service list, 512 -- A maintenance screen, 601 -- The mode setting by the side of service enjoyment, mode registration, an operation system, 602, 606 [-- The equipment failure by the side of service enjoyment, mode switching, mode registration, 608 / -- An inspection, report service.] -- The mode registration by the side of service provision, 603,607 -- A registration confirmed, 604 -- Supervisory service, 605

---

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－111745
（P2002－111745A）
(43)公開日　平成14年４月12日(2002.4.12)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　11/20	Ｂ	５Ｋ０３０
12/46		11/00	３１０Ｃ	５Ｋ０３３
12/28		11/20	１０２Ｄ	
12/56				

審査請求　未請求　請求項の数17　ＯＬ　（全 14 頁）

(21)出願番号　特願2000－302819(P2000－302819)

(22)出願日　平成12年９月29日(2000.9.29)

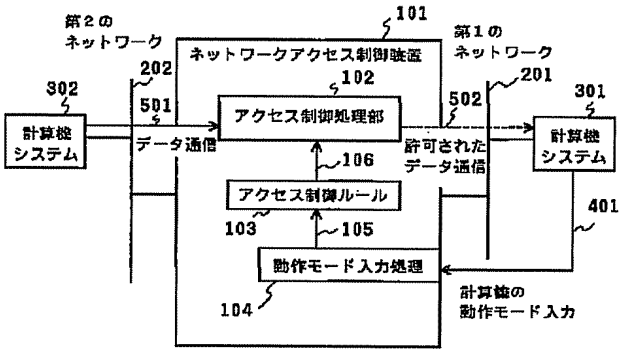
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　浪岡　良光
茨城県日立市大みか町五丁目２番１号　株式会社日立製作所情報制御システム事業部内
(72)発明者　宮尾　健
茨城県日立市大みか町五丁目２番１号　株式会社日立製作所情報制御システム事業部内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　ネットワークアクセス制御装置，その制御方法，その制御システム及び通信サービス方法

(57)【要約】
【課題】計算機を遠隔地から保守する場合に、保守員が保守作業時に使用できるサービスを、保守員自身で各計算機毎に確認できる手段を提供することが課題である。また別の課題として、ネットワークアクセス制御装置において、複数の計算機に対して、該計算機の動作モードにしたがい通信データの通過又は不許可を制御することが課題である。
【解決手段】遠隔から保守することを可能とする計算機と外部ネットワークとの接続ポイントにネットワークアクセス制御装置を設け、該ネットワークアクセス制御装置に該計算機のアクセス制御ルールに対応する動作モードを設けることを特徴とする。複数の計算機からなる計算機の場合には、個々の計算機に対して動作モードを設けることを特徴とする。

図　1



1

【特許請求の範囲】

【請求項１】ネットワークに接続された計算機間の通信制御を行うネットワークアクセス制御装置において、接続されたネットワーク間で通信するデータを制御するアクセス制御ルールと管理する計算機に適用する運用方針を表すモードとを対応させて管理するアクセス制御ルール管理部と、該計算機に適用したモードに対応するアクセス制御ルールを適用してそれに従いコネクションを管理するコネクション管理部と、コネクションを許可した場合のみ複数のネットワーク間で通信データを転送するデータ通信部とを有するネットワークアクセス制御装置。

【請求項２】請求項１において、適用されているアクセス制御ルールを一括して無効化した後、あらかじめ用意した複数のアクセス制御ルールの中から特定のモードに対応するアクセス制御ルールを一括して有効にするコネクション管理部を有することを特徴とするネットワークアクセス制御装置。

【請求項３】請求項２において、適用されているアクセス制御ルールを一括して変更する際、既に確立されていたコネクションについては無効化対象であってもコネクションを継続するコネクション管理部を有することを特徴とするネットワークアクセス制御装置。

【請求項４】ネットワークに接続された計算機間のデータ伝送を制御するネットワークアクセス制御方法において、データ通信条件を規定するアクセス制御ルールに対応し運用方針を表すモードを管理する計算機に適用し、該モードに対応したアクセス制御ルールと受信したデータとを照らし合わせ、通過許可を判断しデータを送出するネットワークアクセス制御方法。

【請求項５】ネットワークに接続された計算機間のデータ伝送を制御するネットワークアクセス制御方法において、接続されたネットワーク間で伝送するデータを制御するアクセス制御ルールと管理する計算機に適用する運用方針を表すモードとを対応させるモード対応表と、管理する計算機と該モードとを対応させる計算機対応表と、に基づいて、受信したデータの通過許可を判断し、該データを送出若しくは破棄するネットワークアクセス制御方法。

【請求項６】ネットワークに接続された計算機間のデータ通信を制御するネットワークアクセス制御システムにおいて、データ通信判断の基準となるアクセス制御ルールに対応し運用方針を表すモードを管理する計算機に適用し、該モードに対応したアクセス制御ルールと外部計算機から受信したデータとを照らし合わせ通過許可を判断し、管理する計算機へデータを送出することで通信を制御するネットワークアクセス制御システム。

【請求項７】請求項６において、管理する複数の計算機と該モードを対応させ、それに基づきデータ通信を制御するネットワークアクセス制御システム。

2

【請求項８】ネットワークに接続された計算機間のデータ通信を制御するネットワークアクセス制御装置を介して遠隔操作により行う遠隔保守サービス提供方法であって、サービス享受者がネットワークアクセス制御装置に設定した運用方針を表すモードに応じて、該モードで通信可能なサービスで計算機を保守又は管理する遠隔保守サービス提供方法。

【請求項９】ネットワークに接続された計算機間のデータ通信を制御するネットワークアクセス制御装置を介して遠隔操作により行う遠隔保守サービス提供方法であって、サービス享受者がネットワークアクセス制御装置に設定した計算機に対する運用方針を表すモードに応じて、複数の計算機を該モードで通信可能なサービスで保守又は管理する遠隔保守サービス提供方法。

【請求項１０】ネットワークに接続された計算機間のデータ通信を制御するネットワークアクセス制御装置を介して遠隔操作により行う遠隔保守サービス提供方法であって、サービス享受者がネットワークアクセス制御装置に設定した計算機に対する運用方針を表すモードに応じて、サービス提供者の計算機の画面に該モード又は運用方針を表示し、計算機を保守又は管理する遠隔保守サービス提供方法。

【請求項１１】請求項１０において、サービス内容を保守サービス画面に表示することを特徴とする遠隔保守サービス提供方法。

【請求項１２】請求項１０において、保守又は管理する計算機を保守サービス画面に表示することを特徴とする遠隔保守サービス提供方法。

【請求項１３】請求項８乃至１２において、モードはイニシャルモード，オンラインモード，保守モード，テストモード，モニタランモードのいずれかのうち一つ以上を含む遠隔保守サービス提供方法。

【請求項１４】請求項８乃至１３において、計算機に適用するモードに応じて保守サービス料金を課金する遠隔保守サービス提供方法。

【請求項１５】請求項８乃至１３において、計算機に適用するモードに応じて保守サービス料金を課金する際に、計算機ごとに課金することを特徴とする遠隔保守サービス提供方法。

【請求項１６】ネットワークアクセス制御装置を介して通信する計算機間の遠隔保守サービス方法であって、通信中にサービス享受者がアクセス制御ルールを切り替えても計算機間のコネクションを確立して通信が終了するまで通信を継続しサービスを提供する遠隔保守サービス方法。

【請求項１７】ネットワークアクセス制御装置を介して通信する計算機間のコンテンツ配信サービスにおいて、配信サービスに有効期間を設定してサービス提供する際に、有効期間を過ぎても該期間中に確立された通信は継続してサービスを提供するコンテンツ配信サービス方

法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークアクセス制御装置及び方法，システム並びに遠隔保守サービス方法に関する。

【０００２】

【従来の技術】従来この種のアクセス制御技術は、ルータやファイアウォールと呼ばれる製品として実現されている。従来技術では、予めアクセス制御をするためのルールを設定しておき、そのルールに従い通信データの通過許可又は不許可を制御している。またそのルールは、送信先の計算機のネットワークアドレスを元に通信データの通過許可又は不許可を指定する方式が広く知られている。

【０００３】また計算機を遠隔から保守する技術について、計算機に動作モードとして保守モードを設け、該計算機自身で保守モードを判定し、保守モードで許可された通信データを受信し、保守モードでは許可されていない通信データを受信しないことで、誤ったデータを計算機が受信しないようにするアクセス制御技術は広く知られている。

【０００４】従来のネットワークアクセス制御装置には、計算機間で通信するデータの単位であるパケットごとに転送先または転送元を調べ、予め与えられた規定に基づき転送を行うパケットフィルタリング装置が広く知られている。また、通信を行う業務アプリケーションプログラムに特化し、データの通信手順や通信するデータの種類に対して通信条件の規定を設け、それに基づき転送を行う通信代行装置が広く知られている。

【０００５】また、転送可否を規定するルールを動的に変更する装置としては、特開平１１－１６７５３８号に記載のように、個々のルールを順次適用するものとなっていた。

【０００６】

【発明が解決しようとする課題】しかし、ルールを適用するための保守モードを各計算機で設定しては設定が煩雑であり、保守モードを設定できない計算機についてはファイアウォールでルールを設定しなくてはならない。アクセス制御ルール管理において、複数のルールを１つのアクセス制御ルールとしてグループ化し、現在ネットワークアクセス制御装置に適用されているアクセス制御ルールの目的を識別できるようにすることが課題である。

【０００７】そして、複数の計算機へのアクセス制御においてルールを設定する際にどの計算機がどんな運用方針，セキュリティーポリシーであるか掴みにくい。よって、ネットワークアクセス制御装置において、複数の計算機に対して、該計算機の動作モードにしたがい通信データの通過又は不許可を制御することが課題である。

【０００８】計算機を遠隔地から保守する場合に、保守員が保守作業時に使用できるサービスを、保守員自身で各計算機毎に確認できる手段を提供することが課題である。

【０００９】

【課題を解決するための手段】上記課題を解決するために、遠隔から保守することを可能とする計算機と外部ネットワークとの接続ポイントにネットワークアクセス制御装置を設け、該ネットワークアクセス制御装置に該計算機のアクセス制御ルールに対応する動作モードを設けることを特徴とする。複数の計算機からなる計算機の場合には、個々の計算機に対して動作モードを設けることを特徴とする。

【００１０】また、ネットワークアクセス制御装置が保持する動作モードとアクセス制御ルールから、ネットワークアクセス制御装置を介して保守作業時に使用できるサービスを、個々の計算機毎に表示することを特徴とする。

【００１１】

【発明の実施の形態】本発明の実施例１として、計算機の動作モードを入力し、該モードにしたがいアクセス制御を実施する例を図１に示す。第１のネットワーク（２０１）、および第１のネットワークに接続された計算機（３０１）、また第２のネットワーク（２０２）、および第２のネットワークに接続された計算機（３０２）が存在し、ネットワークアクセス制御装置（１０１）は第１のネットワーク（２０１）と第２のネットワーク（２０２）を接続している構成である。ネットワークアクセス制御装置（１０１）は、アクセス制御処理部（１０２），アクセス制御ルール（１０３）、および動作モード入力処理部（１０４）からなる。アクセス制御処理部（１０２）は、第２のネットワークに接続された計算機からデータを受信（５０１）し、アクセス制御ルール（１０５）に照らし合わせ（１０６）、該データの通過許可すべきかどうかを判定し、通過許可する場合は第１のネットワークに接続された計算機（３０１）にデータを転送（５０２）する。ネットワークアクセス制御装置（１０１）は、計算機の動作モードを入力するための動作モード入力処理部(１０４)をもち、第１のネットワークに接続された計算機(３０１)から該計算機の動作モードを入力する（４０１）。入力された動作モードにしたがって、アクセス制御ルールを該動作モード用に変更（１０５）する。この方法により、第１のネットワークに接続された計算機（３０１）の動作モードにしたがい、通信データの通過許可又は不許可の制御をネットワークアクセス制御装置において実施することができる。たとえば、オンラインモードの計算機(３０１)に対して、オンラインモードでは処理しない試験用の通信データをネットワークアクセス制御装置で廃棄させることが可能となる。

【００１２】ここで、図１におけるアクセス制御処理部（１０２）と変更前後のアクセス制御ルール（１０３）は、図２に示す構成にて実現される。ネットワークアクセス制御装置（１０１）において、アクセス制御処理部（１０２－１）は、データ通信部（１０２－２）と、コネクション管理部（１０２－３）から成る。データ通信部（１０２－２）は、第２のネットワーク（２０２）に接続された計算機（３０２）から、第１のネットワーク（２０１）に接続された計算機（３０１）に対して送信すべきデータを転送するためにネットワークアクセス制御装置（１０１）と確立したコネクション（４０４）、およびネットワークアクセス制御装置（１０１）が受付けたデータを計算機（３０２）へ転送するために計算機（３０２）と確立したコネクション（４０３）にて双方向の通信を中継する。コネクション管理部（１０２－３）は、コネクションの確立可否条件が規定されたアクセス制御ルール（１０３－４）に基づきコネクションの接続を制御する。

【００１３】図１で示されるアクセス制御ルール（１０３）は、図２のアクセス制御ルール管理部（１０３－１）にて実現される。アクセス制御ルール管理部(１０３－１)は、識別子（１０３－２）を持つ複数のアクセス制御ルール（１０３－３）を保持する。

【００１４】図２に示した実現形態の動作について説明する。まず予めアクセス制御ルール（１０３－３）を用意する。アクセス制御ルールは、データ送信元計算機のＩＰアドレスとポート番号、および本発明が搭載されたネットワークアクセス制御装置(１０１)でコネクションを受付けるＩＰアドレスとポート番号、および受付けたデータを送信する、送信先計算機のＩＰアドレスとポート番号を記述する。これらの記述は明示的にコネクションの確立を許可するものであり、ＩＰアドレスまたはポート番号が記述内容に該当しないコネクションは、暗黙のうちにコネクションの確立要求を拒否する。また、アクセス制御ルールには、識別子（１０３－２）を付与する。

【００１５】図１におけるアクセス制御ルール（１０３）の記述フォーマットを、図３に示す。アクセス制御ルールは、プロトコルの種別を示す識別子（１１１）と、コネクションの確立を許可する計算機のＩＰアドレス（１１２）およびポート番号（１１３）、ネットワークアクセス制御装置が受付けるＩＰアドレス（１１４）およびポート番号(１１５)，ＩＰアドレス(１１４)およびポート番号(１１５)で受付けたデータの送信先となる計算機のＩＰアドレス（１１６）およびポート番号（１１７）から成る。

【００１６】図２において、アクセス制御ルール（１０３－３）は、計算機（３０１）または計算機（３０２）の状態にあわせて１つ以上作成し、識別子（１０３－２）を付与する。例えば、計算機（３０１）の動作モードがオンラインであれば、通信が必要な計算機（３０２）からのみコネクションを許可するアクセス制御ルールとし、“オンラインモード”を示す識別子を付与する。例えば、計算機(３０１)の動作モードが保守状態であれば、計算機（３０１）の特定のポートにのみ計算機（３０２）からコネクションを許可するアクセス制御ルールとし、“保守モード”を示す識別子を付与する。例えば、計算機（３０１）の動作モードが試験モードであれば、試験に必要な通信を許可するアクセス制御ルールとし、“試験モード”を示す識別子を付与する。

【００１７】アクセス制御ルール管理部（１０３－１）は、システム管理者もしくは他のプログラムからの指示、例えば図１におけるアクセス制御ルール変更指示（１０５）により、保持しているアクセス制御ルールの中から、指定された識別子を持つ特定のアクセス制御ルール（１０３－４）を、コネクション管理部(１０２－３)へ提示する。

【００１８】コネクション管理装置(１０２－３)は、それまで適用していたアクセス制御ルールの内容を全てを無効にした後、次に適用すべきアクセス制御ルール（１０３－４）を有効にする。ここで、直前のアクセス制御ルールが無効となったことにより、既に確立されているコネクションも無効となる場合には、計算機(３０１)または計算機（３０２）のいずれかが明示的にコネクションを切断しない限り、そのコネクションは継続されるものとする。

【００１９】計算機（３０２）からネットワークアクセス制御装置（１０１）へコネクションの要求があった場合、コネクション管理部（１０２－３）は、要求に含まれている計算機（３０２）のＩＰアドレスとポート番号の情報を取得し、現在有効となっているアクセス制御ルール（１０３－４）の中から、図３に示すＩＰアドレス（１１２）とポート番号（１１３）が合致する記述を検索する。合致する記述が無い場合は、コネクション要求を拒否する。合致する記述が存在する場合、コネクション管理部（１０２－３）は、検索された記述の中で図３に示す転送先計算機のＩＰアドレス（１１６）とポート番号（１１７）に対してコネクションを確立する。以降、図２の計算機（３０１）または計算機（３０２）のいずれかが明示的にコネクションを切断するまでコネクション（４０３）とコネクション（４０４）を継続し、確立したコネクションで受付けたデータはデータ通信部（１０２－２）が中継する。

【００２０】アクセス制御ルール管理部（１０３－１）は、システム管理者あるいは他のプログラムからの指示により、コネクション管理装置が適用しているアクセス制御ルール（１０３－４）の識別子を提示する。

【００２１】なお、データ通信方式には、単一のポート番号だけでなく、ＦＴＰのように通信途中から任意のポート番号を使用してデータ通信を実現する方式も存在す

る。その場合の動作を図４に示す。計算機（３０１）と計算機（３０２）が通信する際、計算機（３０２）がネットワークアクセス制御装置（１００）の特定のポート番号にコネクションを確立する（２１０－２）。ネットワークアクセス制御装置（１００）は、アクセス制御ルールに従い、計算機（３０１）とのコネクションを確立する（２１０－１）。計算機（３０１）は、現在使用可能な任意のポート番号をネットワークアクセス制御装置（１００）に送信する（２１１－１）。ネットワークアクセス制御装置（１００）は、計算機（３０１）と同様、自身が現在使用可能な任意のポート番号を計算機（３０２）へ送信する（２１１－２）。ここで、ネットワークアクセス制御装置（１００）は、自身が選択した現在使用可能な任意のポートへのコネクション要求を許可するものとすることで、先のポート番号に対して計算機（３０２）がコネクションを要求してきた時点でも継続してコネクションを確立することができる。

【００２２】本発明の実施例２として、計算機の動作モードとして保守モードを適用した例を図５に示す。第１のネットワーク（２０１）に計算機１（３０１－１），計算機２（３０１－２），計算機３（３０１－３）が接続され、計算機はそれぞれ動作モードを持つ。計算機１（３０１－１）の動作モードは保守モードであり、該動作モードの情報をネットワークアクセス制御装置（１０１）の動作モード入力処理部（１０４）に入力（４０１－１）する。また、計算機３（３０１－３）の動作モードはオンラインモードであり、該動作モードの情報をネットワークアクセス制御装置（１０１）の動作モード入力処理部（１０４）に入力（４０１－２）する。第２のネットワークに接続された計算機（３０２）が第１のネットワークに接続された計算機１にデータ通信する場合に、ネットワークアクセス制御装置（１０１）では、アクセス制御ルール（１０３）にしたがい保守モードの計算機に対して許可されたデータかどうかを判定し、許可されたデータである場合に限り計算機１にデータ通信する（５０２）。同様に、計算機３に対してデータ通信する場合には、オンラインモードの計算機に対して許可されたデータかどうかを判定し、許可されたデータである場合に限り計算機３にデータ通信する。

【００２３】本発明の実施例３として、ネットワークアクセス制御装置の実装例について図６～図７に示す。ネットワークアクセス制御装置（１０１）は、アクセス制御処理部（１０２），アクセス制御ルール（１０３），動作モード入力処理部（１０４）からなる。アクセス制御処理部はアクセス制御を実行するプログラム（１０２－４）からなる。アクセス制御プログラム（１０２－４）は、外部からのデータを受信（５０１）し、アクセス制御ルールを記述したデータを読み込み（１０６）、該ルールと通信データを照らし合わせ、許可されたデータの場合にはデータを中継し（５０２）、許可されていないデータの場合にはデータを廃棄する。動作モード入力処理部（１０４）は、動作モード入力プログラム（１０４－１）からなり、計算機からの動作モード入力（４０１）待ちで、いつでも動作モードが入力可能となっている。ある計算機から動作モードが入力されると、該動作モードの情報をアクセス制御ルールに反映し、アクセス制御ルールを変更する（１０５）。図７は、動作モードを入力するための、計算機から動作モード入力処理部へのデータフォーマット（４０１－３）の例である。送信元計算機のネットワークアドレス（４０１－４），ネットワークアクセス制御装置のネットワークアドレス（４０１－５）、および送信元計算機の動作モード情報からなる。計算機は、送信元計算機のネットワークアドレス（４０１－４）により特定できる。動作モードは、送信元計算機の動作モード情報（４０１－６）で指定する。動作モードの例としては、オンラインモード，保守モード，テストモードなどが挙げられる。

【００２４】本発明の実施例４として、計算機を遠隔保守する場合のアクセス制御方式について図８に示す。ネットワークアクセス制御装置（１０１）は、第１のネットワーク（２０１）に接続された計算機（３０１）から動作モード（４０１）を入力し、該動作モードによりアクセス制御ルール（１０３）を変更する。第２のネットワーク（２０２）に接続された計算機（３０２）は、ネットワークアクセス制御装置（１０１）から動作モード（４０１）とアクセス制御ルール（１０３）を入力（４０２）する。計算機（３０２）は、アクセス制御ルール（１０３）の中から、計算機（３０２）のＩＰアドレスが図３で示した送信元計算機のＩＰアドレス（１１２）に合致するルールを検索し、該検索結果から更に図３で示した送信先計算機のＩＰアドレス（１１６）とポート番号（１１７）を抽出してサービス一覧（５１１）を作成する。抽出した情報は、言い換えれば、保守員がネットワークアクセス制御装置（１０１）を介して通信可能な計算機（３０１）および異なる計算機（３０３）について各々保守で使用できるサービスを示している。保守員は、サービス一覧に基づいて表示された保守画面（５１２）にてサービスの使用可否を閲覧する。図９において保守画面（５１２）の構成と動作を説明する。保守画面（５１２）は、動作モード表示部（５２１）と、計算機表示部（５２２）と、サービス表示部（５２３）で構成する。動作モード表示部（５２１）には、図８で示したネットワークアクセス制御装置（１０１）から入力した動作モードを表示する。計算機表示部（５２２）には、図８で示したサービス一覧で得たＩＰアドレスを表示する。また、サービス一覧（５２２）に複数の計算機がある場合は、複数のＩＰアドレスを表示する。保守員は、計算機表示部（５１１）から単一のＩＰアドレスを選択操作する。サービス表示部（５２３）には、選択されたＩＰアドレスについて、図８で示したサービス一覧（５１

１）から得たポート番号を表示する。サービス一覧（５１１）の中に、保守員が選択したＩＰアドレスについて複数のポート番号がある場合は、複数のポート番号を表示する。

【００２５】本発明の実施例４については、計算機一覧表示部（５２２）に関して、ＩＰアドレスに加えて予めＩＰアドレスに関連付けて定義された計算機名を表示してもよい。サービス表示部（５２３）に関して、ポート番号に加えて予めポート番号と関連付けられたサービス名を表示してもよい。また、アクセス制御ルール（１０３）は、予め計算機（３０２）にて保持することで、ネットワークアクセス制御装置（１０１）から動作モードだけを入力（４０２）し、サービス一覧（５１１）を作成してもよい。さらに、計算機（３０２）から計算機（３０２）のＩＰアドレスを入力した後、サービス一覧（５１１）をネットワークアクセス制御装置にて作成し、計算機（３０２）へ送信することで、計算機（３０２）は、保守画面（５１２）を表示することもできる。

【００２６】図１０は遠隔保守サービスをサービス提供側とサービス享受側のシステム全体例である。ある設備とそれを制御する計算機があり、ネットワークアクセス制御装置を介して外部へ通信回線を通じて繋がっている。そして保守サービス側の計算機が保守サービスサーバやネットワークアクセス制御装置を介して計算機や設備へと通信できるようになっている。遠隔保守サービスはポートに対応するプロトコル、そしてそのプロトコルのアプリケーションで提供する設備の保守管理作業や修理，情報提供などである。アウトソーシングでの管理に際し、Ａ社とＢ社の設備が使われていたとき、管理をそれぞれの会社で行わせたい場合には、それぞれの会社に対応するモードを設定することにより、簡単に設定、運用ができる。設備としては、発電設備や工場生産ラインなどの産業プラントなどが挙げられる。

【００２７】図１１はサービスを行う上でのフローの例である。サービス享受側の計算機にオンラインモードを設定し、これによりプロセス制御が行われ設備が運転を開始する。計算機に設定されたモードはネットワークアクセス制御装置に登録される。この登録作業は計算機にモードが設定された際に計算機からネットワークアクセス制御装置に送信する（６０１）。そしてネットワークアクセス制御装置への登録内容が変わったことを保守サービスサーバへと伝え登録する（６０２）。オンラインモードでは通常の運転状態でプラント制御が行われているので、制御している計算機の状態を変更して致命的なミスを冒さないように通信制御ルールを設定しておく。保守員は登録されたオンラインモードでできる保守を行う。ここでは監視サービスであり、異常がないかどうか監視している（６０４）。設備が故障した場合は設備が故障したのを計算機が検知し、オンラインモードから保守モードへと切り替わる。保守モードはプログラムの入れ替えやデータの変更など、計算機の動作を変更させるための作業ができる状態になるように制御ルールが設定されている。計算機はモード変更をネットワークアクセス制御装置に登録し（６０５）、ネットワークアクセス制御装置は保守サービスサーバへ計算機のモード変更を登録する（６０６）。これにより今までオンラインモードで監視していた保守員は保守モードへと登録が変更になったのを確認し（６０７）、異常があったことを知り、保守モードでできる保守検査を行いその結果を報告する（６０８）。

【００２８】ここではモード変更の度に保守サービスサーバへ登録しているが、登録せずに通信する際にモードの情報を通信しても良い。

【００２９】保守モード以外の計算機には保守モードデータが行かないようにすることにより、遠隔から操作を許可された者が誤って保守モード以外の計算機に対して通信データを送信することを防ぐことができる。

【００３０】設備が故障したのを計算機が検知するものを挙げたが、作業員による入力の他に、保守サービスの監視において異常を確認し、保守サービス側の計算機から、保守計算機のモードを変更できるようにしてもよい。この時は、ファイアウォールであるネットワークアクセス制御装置内のモードを扱うことになるのでセキュリティの観点から他の暗号化技術などを併用する必要がある場合も考えられる。これによりネットワークアクセス制御装置において、該装置の管理者の操作なしにアクセス制御ルールを変更することができる。

【００３１】図１２は保守サービスの料金の課金方法の一例を示す。モードを設定し保守サービスを依頼すると、保守サービス提供側はそのモードでできるサービスでの保守管理を行う。サービス毎にある時間当たりの料金を決めておき、そのサービスで費やした時間より料金を決定し課金する。モードを変更することによりサービス内容が変わるので、受けたいサービスを受けたい時に、そのサービスに見合った料金で受けることができる。また、計算機ごとにモードを設けることにより各計算機ごとに料金を変えても良い。他の課金方法としては月極など一定期間に一定料金にする方法がある。

【００３２】ルールとモードを対応させる例として図１３の様に対応させ、ネットワークアクセス制御装置で管理される。ネットワークアクセス制御装置でルールとモードを対応させ管理することにより、各計算機でモードを設定できなくとも良くなり、ネットワークアクセス制御装置にてルールを適用することにより各計算機には必要な情報だけを流すことができる。そのため、各計算機で必要な情報かどうかを判断しなくても良くなるので各計算機の負荷が減る。運用方針を表すモードを複数設けることにより、運用方針を変更することで適用したいルールを一度に、手間無く入れ替えることができる。

【００３３】また、各計算機とそのモードを対応させる

例として図１４の様に対応させ、ネットワークアクセス制御装置で管理される。各計算機毎にモードを設定することにより、各計算機の運用方針を把握しやすく簡単にルールを適用できる。１台の計算機から複数の計算機に対して、動作モード毎のアクセス制御ルールが適切に定義されているか否かを確認することもできる。いくつかの計算機を運用方針上おなじ計算機群としてモードと対応させることにより、計算機群のシステムの運用方針としてまとめることもできる。

【００３４】モードの代表的な例としては以下の様なものが挙げられる。

（１）イニシャルモード：計算機を起動したとき、業務用アプリケーション（プラント制御プログラムなど）を実行しない状態。この状態から、他のモードへ遷移する。

（２）オンラインモード：業務用アプリケーションが起動され、プラント制御を行う。通常の運転状態。

（３）保守モード：プログラムの入れ替えやデータの変更など、計算機の動作を変更させるための作業ができる状態。

（４）テストモード：計算機が最終的な制御命令を出さない状態。制御機器からのデータ受信と制御命令の送信を擬似的に行う。動作試験時に使用する。

（５）モニタランモード：テストモードとは異なり、制御機器からのデータ受信は実際のプラントから受信する状態。動作試験時に使用する。

【００３５】複数のモードを切り替えることにより管理する計算機または保守する計算機に対するアクセス制御ルールを変更できるので、管理運用方針を把握しつつ簡単にルールを適用できる。

【００３６】保守サービスは例に挙げたモードやサービス内容に囚われず、必要なモードを適宜作成し、多様なサービスを実施することが必要である。

【００３７】図１５はルール一括適用の流れを表す例である。ネットワークアクセス制御装置をあるモードから別のモードへと切り替えるとき、新しいルールを３つ適用する。外部からのコネクション要求が来ている際にルール３つを順次適用していくが、上段はルールを一括適用しない場合であり、下段はルールを一括適用する場合である。外部との通信において通信Ａと通信Ｃを必要とするとき、上段の状態Ａ及び状態Ｂでは通信Ａのみがコネクションを確立し通信でき通信Ｃがコネクションを確立できていない。これに対し下段のルールを一括適用する場合は、モードによるルールセットが適用されてから通信を開始するので通信Ａと通信Ｃの通信の整合性が良い。管理している計算機に適用されているアクセス制御ルールを一括して無効化した後、適用したい運用方針を表す識別子であるモードと対応する複数のアクセス制御ルールを一括して有効にすることにより、アクセス制御ルールが複数のルールから成る場合、個々のアクセス制御ルールを順次変更していくことによる過渡状態を発生させずにアクセス制御ルールを動的に変更させることができる。

【００３８】図１６はルール適用とコネクション継続の例である。外部からのコネクション要求が来ると、親プロセスは通信先の計算機に適用されているモードのルールセットにより通信可否を判断し、通信可であれば、子プロセスに通信の仕事を渡す。子プロセスはコネクション要求に対してコネクションを確立し、通信し、通信が終了するとクローズする。子プロセスは親プロセスから仕事である通信を受けるときに生成される場合もあれば、最初から在る場合もある。

【００３９】親プロセスは通信先計算機のルールセットが適用される途中でコネクション要求があった際には、ルールセットが適用され終わってから子プロセスへと仕事を受け渡すことによりルールを一括適用できる。また、子プロセスは一度コネクションを確立したら、コネクションをクローズするまで通信を続け、クローズすると親プロセスに対して仕事待ちの状態になる。通信の途中でのルール適用をしないことにより、コネクションを確立した通信が通信の途中でルールが入れ替わることによるコネクションのクローズで通信できなくなることが無い。

【００４０】従来技術を用いたパケットフィルタリング装置では、通信を拒絶するアクセス制御ルールが適用された時点でパケットの転送が行われなくなるため、転送が中断されたことを業務アプリケーションプログラムが検知し、それまでのデータあるいはそれに対する一連の処理すべてを無効にしなければならないことがある。しかし、適用されているアクセス制御ルールを変更する際、既に確立されていたコネクションについては無効化対象であってもコネクションを継続することにより、処理の連続性を確保できる。これにより、アクセス制御ルールを一括して切り替えることによって、通信中にアクセス制御ルールを切り替えても計算機間のコネクションを確立して通信が終了するまで通信を継続しサービスを提供することができる。

【００４１】遠隔保守サービスにおいて、通信のコネクションが確立されてからクローズするまでの時間でサービス時間としてサービス料金を課金する方法の場合、保守サービス作業の途中でコネクションが切断されると途中までの作業が無駄になり、再度やりなおさなくてはならない。このとき、保守サービス提供側としては作業の手間数が増え、サービス享受側としては作業時間の増大により料金が増えてしまう。また、音楽配信などでコンテンツプロバイダからデータを配信するサービスにおいて、コンテンツを提供する期間を定めて課金するとき、サービス提供側ではクライアントのサービス期間の終了に伴いルールを変更することが考えられるが、サービス享受側であるクライアントが配信サービス期限の直前か

らコネクションを確立していた場合、通信の途中でコネクションが切られるとその通信は無駄になってしまう。ルールを一括適用し、コネクションを継続させることにより保守サービスや配信サービスにおいてより確実な通信を提供でき、より良いサービスを提供し、サービスに見合った課金もすることができる。

【００４２】

【発明の効果】本発明によると、遠隔から計算機の保守をする場合に、計算機が保守モードである、言いかえると計算機が保守可能状態であることをネットワークアクセス制御装置にて判定し、誤って保守モード以外の計算機に対して保守用のデータを送信することを防止する効果がある。

【００４３】また、現在適用中のアクセス制御ルールを意味的に解釈できるため、システム管理者は適用中のアクセス制御ルールを確認することが容易となり、又、現在使用できるサービスを保守員に示すことで、サービスが可能か否かを調べるための試行作業を行わずに済む効果がある。

【図面の簡単な説明】

【図１】システム構成図。

【図２】アクセス制御処理部とアクセス制御ルール管理部の構成。

【図３】アクセス制御ルールのデータフォーマット。

【図４】複数のポートを使用する通信方式。

【図５】複数計算機からなる計算機の図。

＊【図６】ネットワークアクセス制御装置の構成。

【図７】通信データフォーマット。

【図８】遠隔保守作業でのアクセス制御方式。

【図９】保守画面の構成。

【図１０】遠隔保守サービスの全体図。

【図１１】保守サービス側とサービス享受側のフロー。

【図１２】保守管理サービス料金の課金のフロー。

【図１３】動作モードとアクセス制御ルールの対応表。

【図１４】計算機と動作モードの対応表

【図１５】ルール一括適用の流れ。

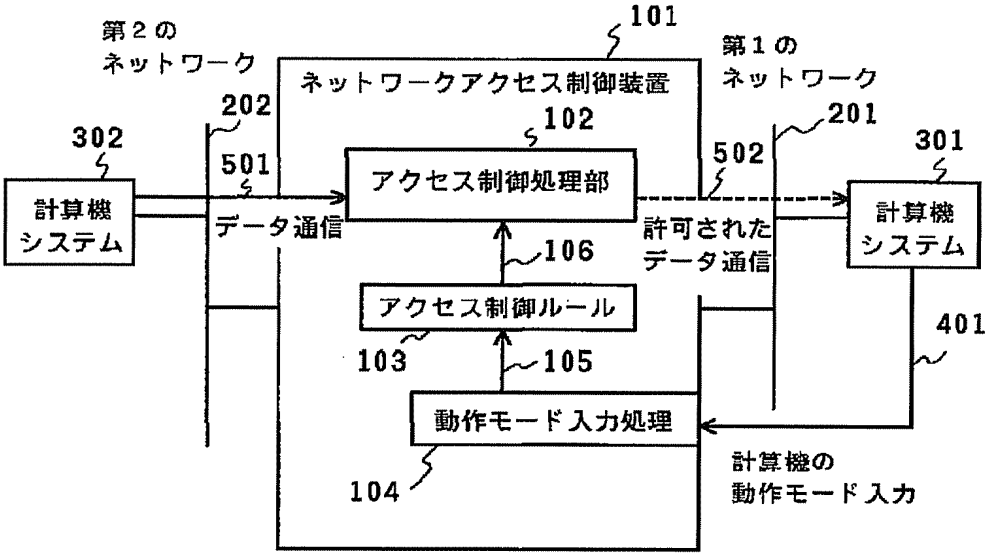
【図１６】ルール適用とコネクション継続の例。

【符号の説明】

１０１…ネットワークアクセス制御装置、１０２…アクセス制御処理部、103…アクセス制御ルール、１０４…動作モード入力処理部、１０５…ルール変更、１０６…データ読み込み、２０１～２０２…ネットワーク、２１０…コネクション確立、２１１…ポート番号送信、２１２…通信、３０１～３０２…計算機、４０１～４０２…動作モードの入力、５０１～５０２…データ通信、５１１…サービス一覧、５１２…保守画面、６０１…サービス享受側のモード設定，モード登録，設備運転、６０２、６０６…サービス提供側へのモード登録、６０３，６０７…登録確認、６０４…監視サービス、６０５…サービス享受側の設備故障，モード切り替え，モード登録、６０８…検査，報告サービス。

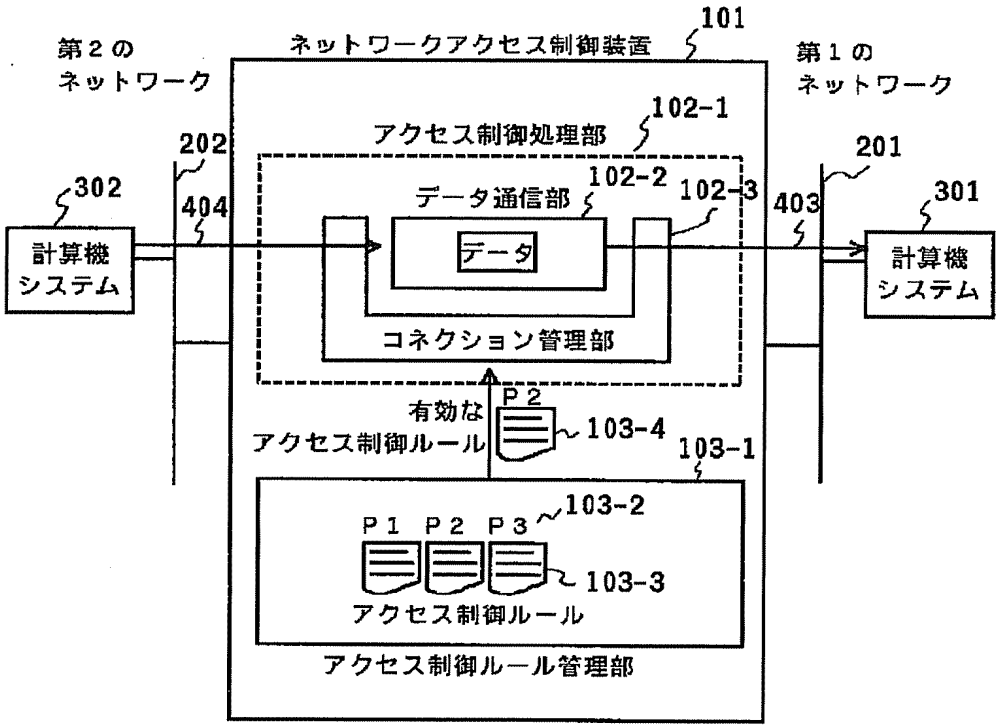
【図１】

図　１



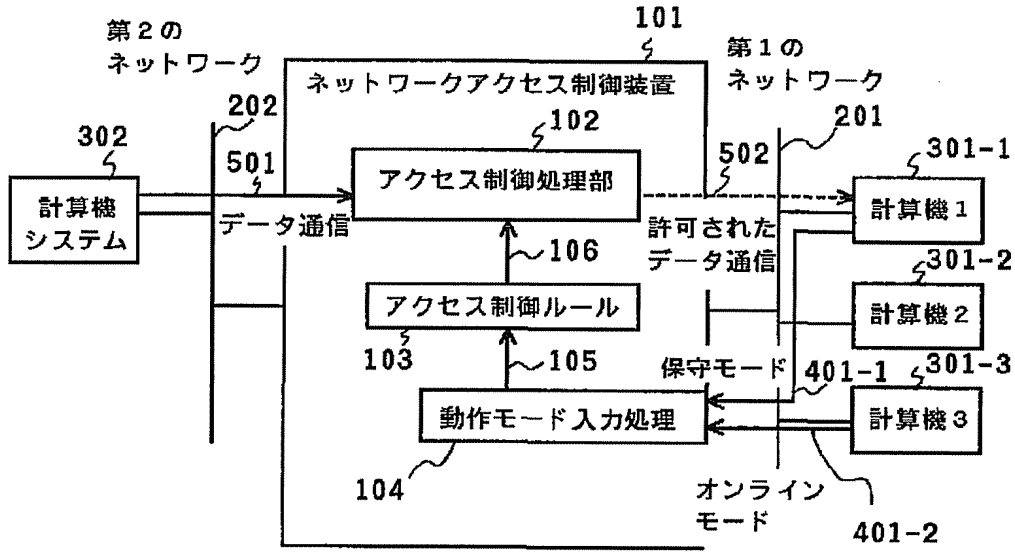
【図２】

図　２


101
第２の
ネットワーク
ネットワークアクセス制御装置
第１の
ネットワーク
102-1
アクセス制御処理部
202
201
302
102-2
102-3
データ通信部
404
403
301
データ
計算機
システム
計算機
システム
コネクション管理部
有効な
アクセス制御ルール
P２
103-4
103-1
P１ P２ P３
103-2
103-3
アクセス制御ルール
アクセス制御ルール管理部

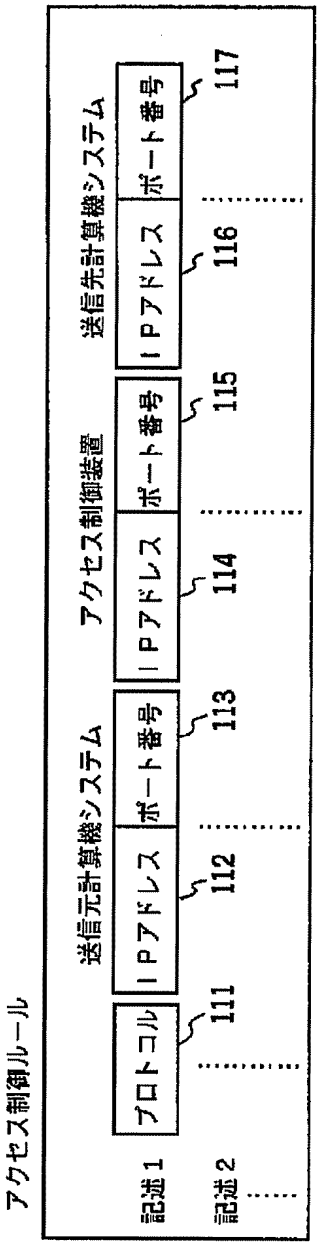
【図５】

図　５


101
第２の
ネットワーク
ネットワークアクセス制御装置
第１の
ネットワーク
202
102
201
302
501
502
301-1
アクセス制御処理部
計算機
システム
データ通信
許可された
データ通信
計算機１
106
301-2
アクセス制御ルール
計算機２
103
105
保守モード
401-1
301-3
動作モード入力処理
計算機３
104
オンライン
モード
401-2

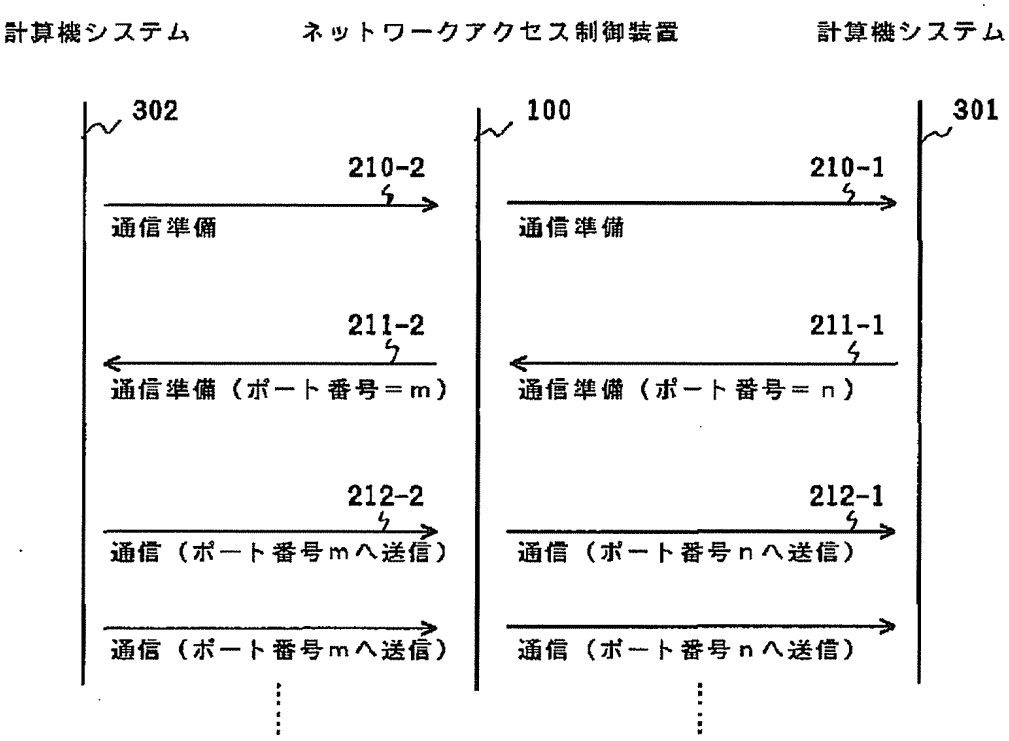
【図３】

図　３


アクセス制御ルール
送信元計算機システム
アクセス制御装置
送信先計算機システム
プロトコル
ＩＰアドレス
ポート番号
ＩＰアドレス
ポート番号
ＩＰアドレス
ポート番号
記述１
記述２
111
112
113
114
115
116
117

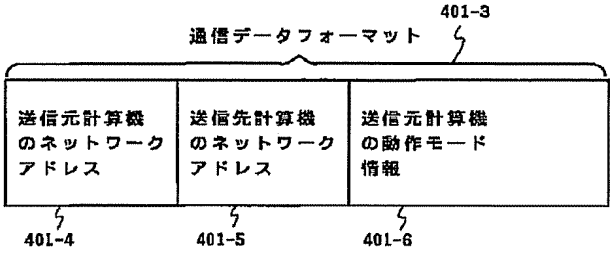
【図４】

図　４



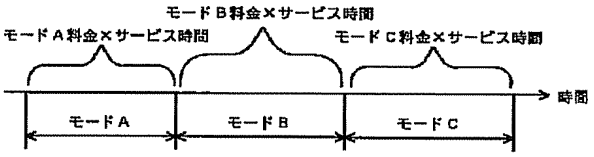
【図７】

図　７



【図１２】

図　12



【図１３】

図　13

動作モード	アクセス制御ルール
モードＡ	ルール１
モードＢ	ルール１、２
モードＣ	ルール３
モードＤ	ルール１、２、３
モードＥ	ルール４

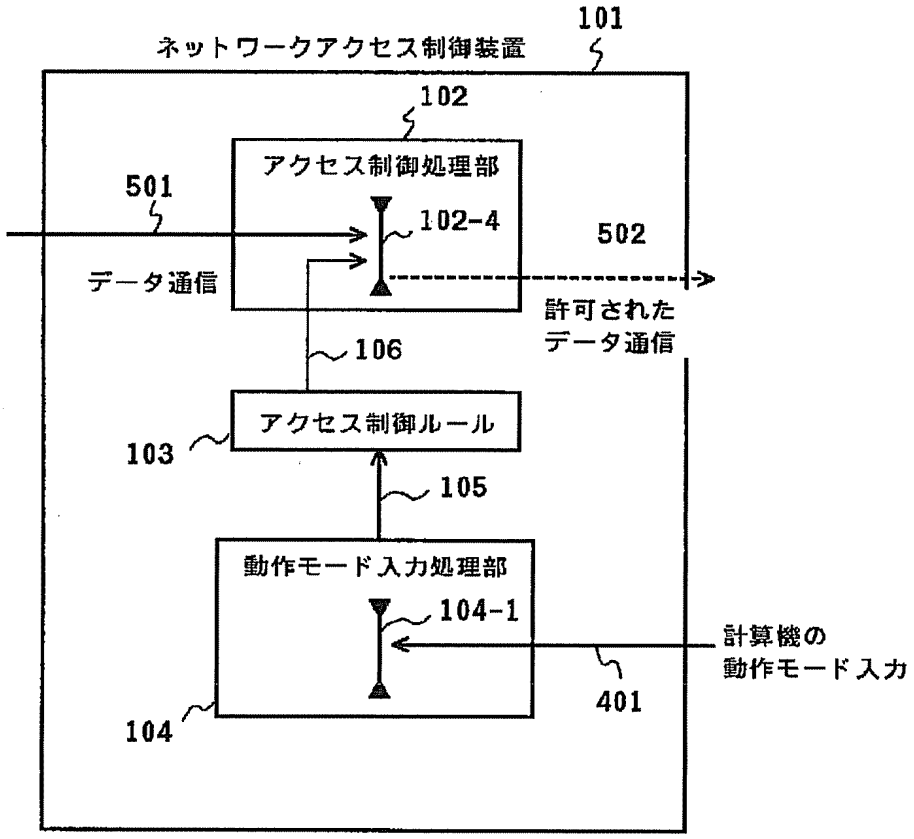
【図１４】

図　14

計算機システム	モード
計算機イ	モードＡ
計算機ロ	モードＡ
計算機ハ	モードＢ
計算機ニ	モードＣ
計算機ホ	モードＣ

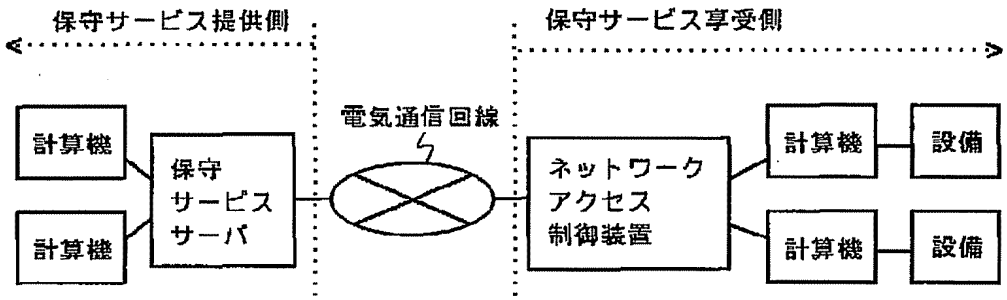
【図６】

図　６


ネットワークアクセス制御装置
101
102
アクセス制御処理部
501
102-4
502
データ通信
許可された
データ通信
106
アクセス制御ルール
103
105
動作モード入力処理部
104-1
計算機の
動作モード入力
401
104

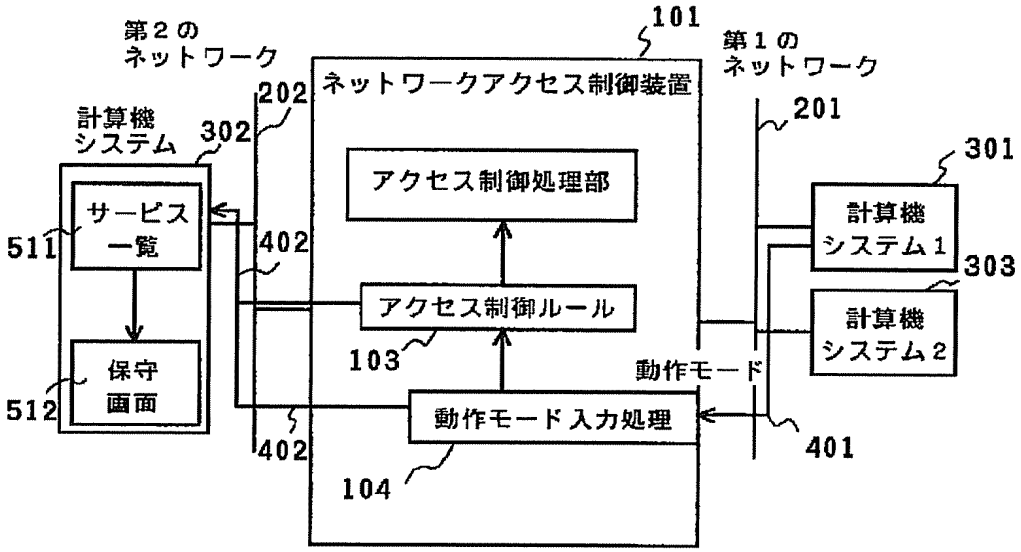
【図１０】

図　10


保守サービス提供側
保守サービス享受側
電気通信回線
計算機
計算機
保守
サービス
サーバ
ネットワーク
アクセス
制御装置
計算機
設備
計算機
設備

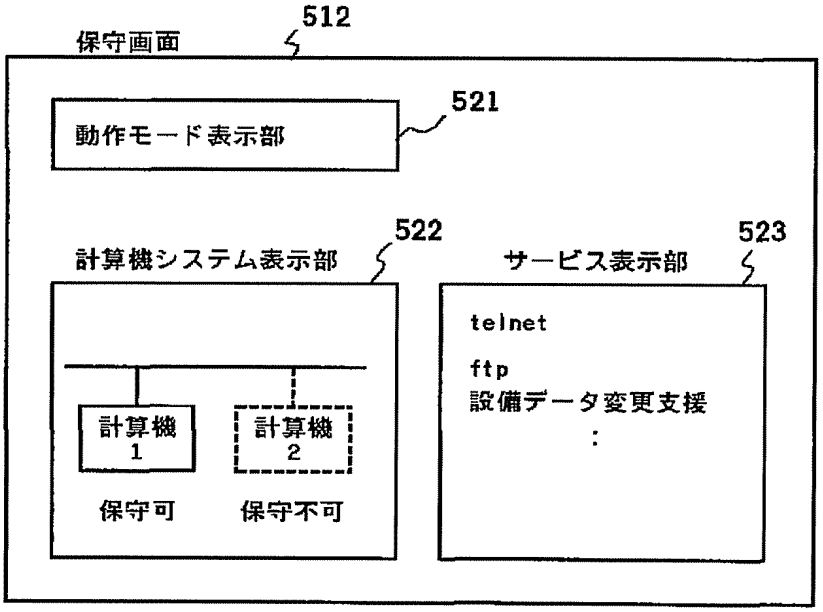
【図８】

図 8


第２の
ネットワーク
101
第１の
ネットワーク
ネットワークアクセス制御装置
202
201
計算機
システム
302
301
アクセス制御処理部
サービス
一覧
511
402
計算機
システム１
303
計算機
システム２
アクセス制御ルール
103
保守
画面
512
動作モード
動作モード入力処理
401
402
104

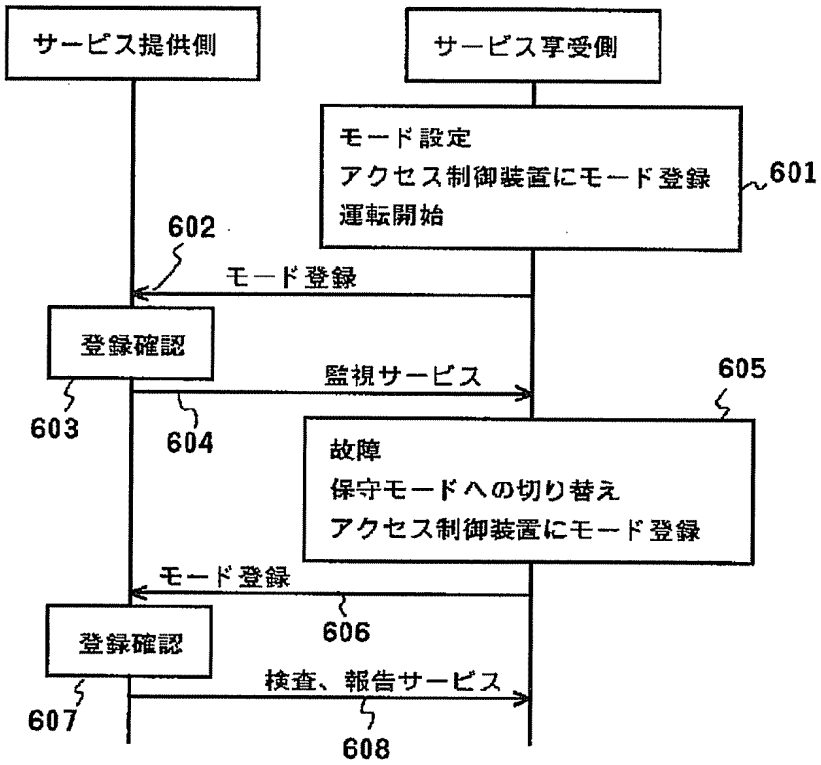
【図９】

図 9


保守画面
512
動作モード表示部
521
計算機システム表示部
522
サービス表示部
523
telnet
ftp
設備データ変更支援
:
計算機
1
計算機
2
保守可
保守不可

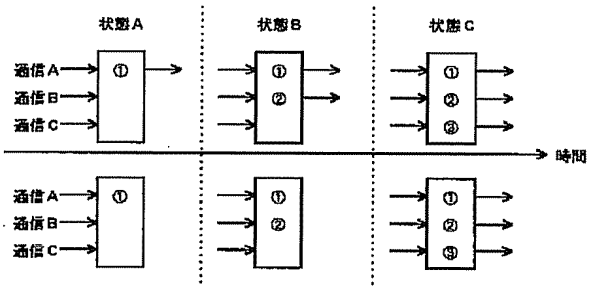
【図１１】

図　11



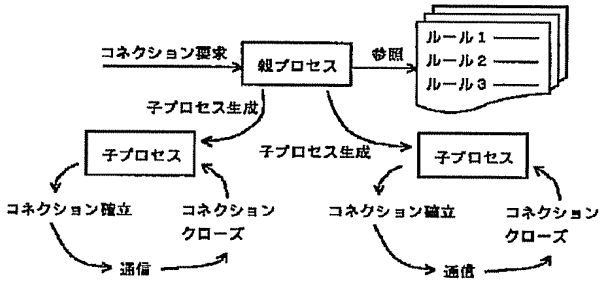
【図１５】

図　15



【図１６】

図　16



フロントページの続き

(72)発明者　中野　利彦
茨城県日立市大みか町五丁目２番１号　株式会社日立製作所情報制御システム事業部内

Ｆターム(参考)　5K030 HA08 HB06 HB08 HD06 JA11
JT06 KA05 LB05 LB19 LC15
5K033 BA04 BA08 CB06 CB08 DA05
DB12 DB14 DB16 DB18 EA07